NASIG Newsletter
Vol. 33, no. 2 May 2018 eISSN 1542-3417

Columns

Standards Corner: Challenges of Identity and Authentication Management, Part One

Emily Ray, Standards Committee

This is the second column of a two-part review on the topic of identity and authentication management as presented in the November 2017 NISO webinar "Engineering Access under the Hood, Part One – Challenges of Identity and Authentication Management."

The previous column covered the first half of the webinar with President of Informed Strategies, Judy Luther's presentation on the current state and challenges of identity and authentication management. This column will cover the presentation by Phil Leahy, describing his work as Service Relations Manager supporting organizations using OpenAthens, and Ellen Rotenberg, Director of Product Management and Rick Stevenson, Manager of Technical Operations at Clarivate Analytics, on the service provider side of authentication and identity management.

Leahy began by talking about the history of OpenAthens, an identity and access management service that is part of Eduserv, a not-for-profit technology organization that works with academic and other organizations in the UK. Originally named "Athens," it first implemented a federated login and later became OpenAthens and grew to be used by 2,000 organizations in 47 countries. It also switched from proprietary code to SAML (Security Assertion Markup Language, an open standard XML-based markup language for exchanging authentication and authorization data) in their process for providing authentication.

Leahy described what he called the components of the "federated access toolkit" – vendor-supplied credentials, referral URLs, peer-to-peer SAML connections, and IP recognitions. Using these tools, federated access management can authenticate users to provide access to desktop and cloud applications, network drives, VLE or LMS services in eLearning, etc. The next step is to authenticate users to access subscription content. In federated access management, the user is directed back to their organization, which could be a university, government agency, or non-governmental organization. The affiliated organization then manages the authentication of their user as the organization has access to all the necessary information, identification, currency, and type of access of the user. Having the affiliated organization authenticate their user in one place is why this method is also called Single Sign On (SSO).

Leahy also discussed the difference between the US and UK in using federated access management. He attributed the greater use of federated access management in the UK to early support and investment by higher education councils. He closed by reviewing some of the advantages of federated access management compared to IP authentication. IP authentication identifies a location, not the user, VPN can work with IP authentication, but there is an additional step for the user, and federated access management can provide better reporting for internal assessment.

Ellen Rotenberg, Director of Product Management, and Rick Stevenson, Manager of Technical Operations at Clarivate Analytics, presented on the service providers' side of identity and authentication management. Rotenberg began with their core tenets of authentication management: provide the right resources to the right users at the right time; confirm the identity of the user and what (content or services) they are authorized to access.

Clarivate Analytics supports IP authentication, as it is still the most common method of authentication, but they prefer Single Sign On (SSO). Clarivate is also looking for ways to make authentication less complicated. In their view, this includes less IP authentication, replaced by SSO, with organizations consistently providing personalized attributes via SAML(for example, an ID or email address), and progressive identity disclosure--smarter ways for the user to progressively identify themselves and their access as needed. Clarivate considers a best practice to only require a higher level of authentication when needed. For example, some Clarivate products require different levels of authentication: Web of Science, Journal Citation Reports, and EndNote.

Stevenson showed a list of challenges with identity management and recommended solutions. Among the potential solutions he listed moving away from IP authentication in favor of SSO, standards in how assertion attributes (IDs or email) are released by organizations, and standards in how service providers should construct WAYFless URLS (direct links without having to authenticate again).

Stevenson also displayed a spreadsheet of SSO technical issues by root cause for six months. Among the problems were outdated metadata, SAML attribute mismatch, service provider IdP configuration error, and personalization attribute error. Stevenson felt these issues demonstrate the complexity of identity and authentication management from the service provider side. However, with increased adoption by service providers and by organizations and with standardization efforts, such as RA 21's examination of authentication processes, access can be improved for users.